

**REMARKS**

Several editorial revisions have been made to the specification. Claims 42, 47 - 51, 54 - 58, and 61 - 64 have been amended. Claims 70 - 79 have been added. No new matter has been introduced with these revisions, amendments, or added claims, which are supported in the specification as originally filed. Claims 1 - 79 are now in the application.

I. Rejection Under 35 U.S.C. §102(a)

Paragraph 4 of the Office Action dated April 29, 2004 (hereinafter, "the Office Action") states that Claims 42 - 44, 51 - 52, and 58 - 59 are rejected under 35 U.S.C. §102(a) as being anticipated by Request for Comments (hereinafter, "RFC") 2660. This rejection is respectfully traversed.

Applicants' independent Claims 42, 51, and 58 specify limitations of "... sending security-sensitive content [in a second message], wherein said security-sensitive content is encrypted using a server-application-selected message encoding scheme that is thereby proposed to said client application and said first portion [of security information on that second message] enables said client application to decrypt said security-sensitive content" (emphasis added).

The cited text from RFC 2660 does not teach this technique for proposing a message encoding scheme while, at the same time, sending content encrypted using that proposed (and server-application-selected) message encoding scheme on the second message of a 2-message exchange (where the client application is able to decrypt the security-sensitive content using

Serial No. 09/415,645

-31-

Docket RSW9-99-084

security information from this second message). Instead, §1.1, "Summary of Features", states that the cryptographic algorithm (a subset of Applicants' "message encoding scheme") is "negotiated". (See lines 2 - 5 of the paragraph that begins "S-HTTP provides full flexibility ...".) In other words, the client and server first agree on the cryptographic algorithm according to RFC 2660, and subsequently exchange messages using that algorithm. This necessarily requires more message exchanges than Applicants' claimed 2-message flow.

Furthermore, §1.3.1, "Message Preparation", states that the "receiver's cryptographic preferences and keying material" (emphasis added) are required for creating an encrypted message. See the first paragraph, bulleted item number 2. Applicants' claimed technique does not use cryptographic preferences of the receiving client application, but instead sends content that has been secured using a message encoding scheme that is being proposed by the server application (after the client application requests, in the first of the 2 messages, that the server application should select the message encoding scheme). While Applicants' approach may use the client's "keying material" (see, for example, p. 48, line 15, where a client nonce is supplied), requesting the server application to choose the message encoding scheme is distinct from also using the client application's "cryptographic preferences", which is taught by RFC 2660. See also line 3 of the final paragraph of §1.3.2, "Message Recovery", where RFC 2660 states that the receiver (i.e., the client) requested particular message processing (using input #2 to the message creation process, which as just discussed, comprises the receiver's "cryptographic preferences").

§3.1, "Options Headers", also states that RFC 2660 contemplates the receiver (i.e., client)

Serial No. 09/415,645

-32-

Docket RSW9-99-084

informing the sender of the encrypted message (i.e., the server) of the receiver's "cryptographic preferences", and further emphasizes that these preferences are something distinct from the receiver's keying material. See the paragraph that begins "There are two kinds of cryptographic options ...". This paragraph states that one kind of cryptographic option is "negotiation options", which convey the receiver's cryptographic preferences, while a second kind of cryptographic option is "keying options" that provide "keying material" (or pointers thereto). The first paragraph of this section also states that the (explicit) negotiation options may be conveyed in an HTTP request message. While Applicants' Claims 42, 51, and 58 may also use an HTTP request message as the "first message", these claims specify that this first message "requests" that a message encoding scheme be "proposed". This is distinct from supplying preferences for negotiation, as taught by RFC 2660.

See also §3.2.1, "Negotiation Overview", which states in the first sentence that "Both parties are able to express their requirements and preferences ..." (emphasis added). This is distinct from Applicants' claimed server-application-selected approach, where a message encoding scheme is proposed to the client on the same message flow that carries content encoded using that proposed scheme.

In view of the above, Applicants respectfully submit that RFC 2660 does not anticipate their independent Claims 42, 51, and 58. Dependent Claims 43 - 44, 52, and 59 are therefore deemed patentable over the reference as well, and the Examiner is respectfully requested to withdraw the §102 rejection.

Serial No. 09/415,645

-33-

Docket RSW9-99-084

## II. Rejection Under 35 U.S.C. §103(a)

Paragraph 6 of the Office Action states that Claims 47 - 48, 50, 54 - 55, 57, 61 - 62, and 64 are rejected under 35 U.S.C. §103(a) as being unpatentable over RFC 2660 in view of the Examiner's Official Notice. This rejection is respectfully traversed.

Applicants have demonstrated, above, that independent Claims 42, 51, and 58 are patentable over RFC 2660. Thus, dependent Claims 47 - 48, 50, 54 - 55, 57, 61 - 62, and 64 are patentable over this art, whether taken singly or in combination with Official Notice. The Examiner is therefore respectfully requested to withdraw the §103 rejection.

## III. Allowable Claims

Paragraph 7 of the Office Action states that Claims 45 - 46, 49, 53, 56, 60, and 63 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form to include all limitations of the base claim and any intervening claims. As demonstrated above, Applicants' independent Claims 42, 51, and 58 are deemed patentable over the references, and thus Applicants respectfully submit that dependent Claims 45 - 46, 49, 53, 56, 60, and 63 are allowable as currently presented.

## IV. Allowed Claims

Paragraph 8 of the Office Action states that Claims 1 - 41 and 65 - 69 are allowed. Newly-added Claims 70 - 74 and 75 - 79 have been created from allowed Claims 65 - 69, and incorporate all limitations from these allowed claims. Thus, added Claims 70 - 79 are deemed

Serial No. 09/415,645

-34-

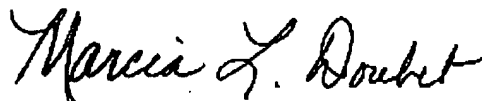
Docket RSW9-99-084

allowable as currently presented.

V. Conclusion

Applicants respectfully request reconsideration of the pending rejected claims, withdrawal of all presently outstanding rejections, and allowance of all claims at an early date.

Respectfully submitted,



Marcia L. Doubet  
Attorney for Applicants  
Registration Nbr. 40,999

Customer Nbr. for Correspondence: 25260  
Phone: 407-343-7586  
Fax: 407-343-7587

Serial No. 09/415,645

-35-

Docket RSW9-99-084